

REMARKS

The claimed invention

The present invention includes methods, computer-executable process steps, and apparatus for encryption of binary data. The methods include iteratively dividing a binary stream into letters or quants to form an alphabet of encryption, which may then be used to create a sequence of logical position scales defining the binary stream. The sequence of logical scales is then concatenated with a coded tag data element, and the process is repeated P times to form an encrypted image.

The cited art

Serpell is directed to a system for the simultaneous generation of identical encryption keys at both ends of a telecommunications link. Transaction keys are produced using a combination of data supplied by a customer and stored by a bank, and data supplied by a retailer.

Gutowitz is directed to a dynamical encryption system based on irreversible dynamical systems (such as cellular automata). The system is disclosed to be well-suited to parallel processing.

Ichikawa is directed to a method of encrypting data with a key and scrambling it, and also encrypting the key using an asymmetrical encryption algorithm. The encrypted key and the encrypted and scrambled data are transmitted to a recipient, who decrypts the key and uses it to decrypt the data.

Campinos is directed to a validation system for ensuring that a service provider's services are usable only by authorized users. The system includes scrambling an item using a series of control words, which are supplied in encrypted messages. A message includes the same control word encrypted with a series of different encryption keys.

Objections to the declaration

The declaration has been objected to for failure to state that the specification has been reviewed and understood, and for failure to acknowledge the Applicants' duty to disclose any material information under 37 C.F.R. § 1.56. The Examiner is directed to page 1 of the declaration, where both of these items appear in the paragraphs immediately following the identification of the serial number of the application.

Objections to the specification

The specification has been objected to for the use of the word “firmness” instead of “security.” Although Applicants believe that the specification would be readily understood in its original form by one of ordinary skill in the art, the term “firmness” has been replaced by “security” throughout the specification with this amendment.

Rejections under 35 U.S.C. § 103

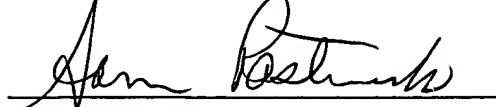
Claims 1-9 and 11-91 stand rejected under 35 U.S.C. § 103(a) as obvious over Gutowitz in view of Campinos and Serpell, and claim 10 stands rejected under 35 U.S.C. § 103(a) as obvious over Campinos in view of Gutowitz, Serpell, and Ichikawa. These rejections are respectfully traversed for the reasons set forth below.

The independent claims of the present application are 1-3 (methods), 35-37 (computer-executable process steps), and 62, 63, and 65 (apparatus). All of these claims have been amended with this response to clarify that the alphabet of transformation AV which is formed during the encryption process is composed of a set of letters or quants which are determined by dividing the binary stream S into segments of bit length m . As discussed in the specification, the alphabet of transformation may simply be the union of all the quants formed by so dividing S (as described in Example 1), or may be a further transformation of that set (as described at page 14, lines 18-29).

None of the cited references describe or suggest the feature of extracting an alphabet of transformation directly from a data stream. The reference relied upon by the Office Action for the existence of an alphabet of conversion is Gutowitz. However, Gutowitz does not extract an alphabet from a data stream, as currently required by all claims. The “alphabet” of Gutowitz is simply a lookup table that allows currency information to be transmitted in a four-bit data structure (rather than using a more conventional coding such as 8-bit ASCII, for example). It is not extracted from the data and plays no part in the actual encryption method. As such, it cannot render the claims as amended obvious. Applicants therefore request reconsideration and withdrawal of the rejections.

Please charge any fees associated with this filing, or apply any credits, to our Deposit
Account No. 03-1721.

Respectfully submitted,

A handwritten signature in black ink, appearing to read "Sam Pasternack", written over a horizontal line.

Sam Pasternack

Registration Number 29,576

Date: December 28, 2004

Choate, Hall & Stewart
Exchange Place
53 State Street
Boston, MA 02109
(617) 248-5000
3783175_1.DOC